Abstract of CN1310526A

Title: INTEGRATED COMPUTER EMERGENCY RESPONSE SYSTEM IN INFORMATION TECHNOLOGY INFRASTRUCTURE AND OPERATING METHOD THEREFOR

A emergency reaction system for network illegal activities of investigation, detection, tracing and evidence obtaining is a safety protection device and method which includes the safety signal converting and transmitting device connected in sequence with the user's end, one or several safety control centres. The present invention utilizes the existing network safety protection products to collect the relevant network safety information and further to form it to be a standard format information to establish VPN channel or encryption channel with the network detecting control centre for transmitting the collected signal to the leadership and transmitting the counter change order from the detecting control centre to the user's end. The present invention can be developed from a single point protection to a system protection, can supply the manual auxiliary handling, can obtain and store the relevant information of network safety event at the same time, can use the system to search out upwards the illegal attack source IP (net work address).

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04B 17/00

[12]发明专利申请公开说明书

[21]申请号 01110293.4

[43]公开日 2001年8月29日

[11]公开号 CN 1310526A

[22]申请日 2001.4.6 [21]申请号 01110293.4

[71]申请人 北京网警创新信息安全技术有限公司
地址 100026 北京市农展南路3号南丰实业公司
[72]发明人 俞 强 孙卫平 赵三华

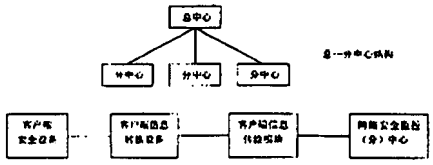
[74]专利代理机构 北京万科园专利事务所
代理人 张亚军 李丕达

权利要求书1页 说明书12页 附图页数4页

[54]发明名称 网络违法行为侦知监控追踪取证应急反应系统及方法

[57]摘要

本发明涉及一种网络系统安全防护装置和方法。它包括依次连接的客户端 安全信息转换和信息传输等设备;一个或多个网络安全控制中心。本发明利用 现有网络安防产品收集网络安全相关信息,并生成标准格式信息,与网络监控 中心建立 VPN 通道或加密通道,向上传输采集的信息,监控中心向下传给客 户端反控指令。本发明可使网络由单点防护发展到系统防护,可支持人工辅助 处理,同时可获取和保存网络安全事件相关资料,并可利用系统上溯查找网络 非法攻击来源 IP(网络地址)。



ISSN1008-4274

01·04·05

权 利 要 求 书

1．一种网络违法行为侦知监控追踪取证应急反应系统，它由客户端和网络安全监控中心设备组成；其特征在于：所述客户端由依次串接的客户端安全设备、客户端信息转换设备和客户端信息传输设备组成；所述客户端安全设备为可以产生与网络状况、网络传输内容有关的信息的软硬件产品或模块，其产生的对安全系统有用的信息被客户端信息转换设备采集处理，将网络安全相关信息转换成网络安全监控中心可以识别的统一格式，再送客户端信息传输设备，所述客户端信息传输设备为双向传送，可向所述网络安全监控中心设备提供安全系统有用的信息和接收反控信息；所述网络安全监控中心设备包括：中心信息传输设备、中心操作平台设备、信息存储设备、信息分析设备和人工支持设备；所述中心操作平台包括标准计算机、显示设备，并且通过中心信息传输设备与各用户端相连接，同时与信息存储设备、信息分析设备和人工支持设备相连接；所述中心信息传输设备可与其他区域中心设备或其他相关系统建立VPN 通道或其他加密传输通道；所述信息分析设备由标准计算机设备构成；所述人工支持设备是供中心操作平台设备访问资料存储库存系统。

2．如权利要求 1 所述的一种网络违法行为侦知监控追踪取证应急反应系统，其特征在于：客户端中，可以一个客户端信息转换设备采集处理多个客户端安全设备产生的信息，也可以是每一个客户端安全设备有一个客户端信息转换设备负责采集处理；一个客户端信息传输设备可以负责一个或多个客户端信息转换设备与网络安全监控中心之间的加密传输。

3．如权利要求 1 所述的一种网络违法行为侦知监控追踪取证应急反应系统，其特征在于：网络安全监控中心可以是由总中心和多个下属分中心连接组成分级中心结构，也可是多个平级的总中心或多级中心连接结构。

4．一种网络违法行为侦知监控追踪取证应急反应方法，其特征在于：利用现有网络安全产品收集客户端网络安全发生事件的各种要素；对所收集的不同格式的信息进行自动识别并生成标准格式的信息，在客户端信息传输设备与网络安全监控中心相应设备之间建立 VPN 通道或其他加密传输通道，保证网络安全监控中心下传给客户端安全设备的反控指令和客户端信息转换设备上传给网络安全监控中心的采集处理的信息在传输过程中不被第三方非法获取或篡改；所述反控信息包括反控指令、设备升级更新程序和查询指令；网络安全监控中心可以与其他相关系统建立加密传输通道，并且可存储传入的信息；该中心进行整个监控区域的调控和重要数据备份与处理。所述监控中心可以是多个分级式或平级式管理模式；所述信息在存储前将进行分级和加密，并设定保留时限及到期处理方式。

说　明　书

网络违法行为侦知监控追踪取证应急反应系统及方法

本发明涉及一种用于广泛监控并制止不同计算机网络间非授权的网络通信和非正常的访问尝试的安全系统及方法。特别是监控并制止一个专用的计算机网络受来自公用网络的非法访问的安全系统及方法。

近来，网络和网络技术的普及已经使得越来越多的敏感信息在与公用网络连接的计算机系统中存储和处理，这些敏感信息包括个人隐私、商务数据、机密文件、重要指令等。如何保护这些信息不被未经授权的外界互联网用户利用网络存在的缺陷非法获取、破坏，如何保护专用计算机网络系统不被外界互联网用户非法进入，已经成为一个重大挑战。如何在专用计算机网络受到外来入侵和攻击时迅速发现并制止，以减少损失，也是网络安全防护的重要课题。

目前用于保护网络安全的产品主要包括防火墙、入侵检测系统（IDS）等。这些网络安全防护产品在用来保护网络安全的过程中仍有一些缺点，表现在：

1. 单一网络安全产品防护技术单一，不同网络安全产品产生的信息不能进行综合。

2. 缺乏对人工参与的支持。现有网络安全产品主要通过正确安装配置后，网络安全产品的软件或者固化在硬件内的程序侦知和阻隔网络违法行为提供网络安全防护。网络安全产品侦知和对抗网络入侵事件时一般不支持人工参与，很少通过实时人机配合的方式对网络提供安全防护。

3. 第三方无法获得产生的相关信息。现有网络安全产品侦知网络违法行为后将产生相关信息，如日志，但这些信息的产生和保存都在用户使用的产品上进行，用户可以进行查阅，但是与第三方（如：政府部门）相关系统之间没有联系，不能作为证据。

4. 没有追踪功能。现有网络安全产品侦知网络违法行为时，可以从相关数据包的中获知来源地址。但是现在的网络犯罪分子经常对自己的地址进行伪装，或者通过代理服务器或者已经被控制的服务器进行中转，隐藏自己的真实网络地址。如果网络攻击者从其他服务器进行中转，数据包中的来源地址就是中转服务器地址，不是攻击者的初始网络地址，无法追踪攻击者（如图一）。

5. 信息来源不广泛。现有网络安全产品只对本地信息进行分析，不能综合其他相关网络中网络安全产品产生的数据进行分析，也不能引入其他系统的有关信息进行分析。进一步决定了现有网络安全产品无法对网络违法行为的真正来源进行有效追踪和分析。例如：现有网络安全产品不支持引入 ISP 的有关记

录信息，从而不能将拨号上网的网络违法行为与拨号使用者直接联系起来。

6. 对于单一用户来说，使用现有网络安全产品的用户数量增加并不能使其网络得到更好的保护，因为现有的网络安全产品只依靠单一产品本身。

本发明的目的是提供一种安全系统及方法，可以随时将一个或多个专用计算机网络内的多个相同或不同网络安全产生的信息进行收集处理，在一个中心及时的综合显示这个或这些专用计算机网络的网络安全状态，通过该安全系统对这些网络安全产品实现远程监控。

本发明的另一个目的是提供一种安全系统及方法，其用来检测网络入侵和提供防护的主要组成单元可以是能从多 来源得到的一般的网络安全产品，而无须采用高成本的特殊网络安全产品。

本发明的另一个目的是提供一种安全系统及方法，在系统内的网络安全产品检测和防止网络入侵时，有关技术人员可以利用本安全系统进行人工参与。

本发明的另一个目的是提供一种安全系统及方法，系统内的网络安全产品产生的信息可以有选择的部分或者无选择的全部向第三方实时或非实时的进行传递。

本发明的另一个目的是提供一种安全系统及方法，可以随时查询该系统内的网络安全产品所处的状态，如：正常工作、无应答、报警等。

本发明的另一个目的是提供一种安全系统及方法，该安全系统可以利用系统获得的和存储的信息进行计算，尝试获得网络攻击的初始网络来源。

本发明的另一个目的是提供一种安全系统及方法，该安全系统可以作为技术平台，当技术人员追查网络攻击的网络来源时提供数据和计算等方面的支持。

本发明的另一个目的是提供一种安全系统及方法，该安全系统不仅可以收集处理网络安全产品产生的信息，而且可以利用其他非网络来源的不同性质的信息，提高该系统的性能。

本发明的另一个目的是提供一种安全系统及方法，该安全系统可以利用其收集的信息进行自学习，发现新的网络攻击模式或新的网络漏洞。

本发明的另一个目的是提供一种安全系统及方法，该安全系统在处理一个专用计算机网络的非法入侵事件时，如果涉及该系统监控的其他专用计算机网络，该系统可以自动采集其他相关专用计算机网络的信息，辅助分析处理。

本发明所述的网络违法行为侦知监控追踪取证应急反应系统由客户端和网络安全监控中心设备组成；其特征在于：所述客户端由依次串接的客户端安全设备、客户端信息转换设备和客户端信息传输设备组成；所述客户端安全设备为可以产生与网络状况、网络传输内容有关的信息的软硬件产品或模块，其产

生的对安全系统有用的信息被客户端信息转换设备采集处理，将网络安全相关信息转换成网络安全监控中心可以识别的统一格式，再送客户端信息传输设备，所述客户端信息传输设备为双向传送，可向所述网络安全监控中心设备提供安全系统有用的信息和接收反控信息；所述网络安全监控中心设备包括：中心信息传输设备、中心操作平台设备、信息存储设备、信息分析设备和人工支持设备；所述中心操作平台包括标准计算机、显示设备，并且通过中心信息传输设备与各用户端相连接，同时与信息存储设备、信息分析设备和人工支持设备相连接；所述中心信息传输设备可与其他区域中心设备或其他相关系统建立 VPN 通道或其他加密传输通道；所述信息分析设备由标准计算机设备构成；所述人工支持设备是供中心操作平台设备访问资料存储库存系统。

如上所述的系统，其特征在于：客户端中，可以一个客户端信息转换设备采集处理多个客户端安全设备产生的信息，也可以是每一个客户端安全设备有一个客户端信息转换设备负责采集处理；一个客户端信息传输设备可以负责一个或多个客户端信息转换设备与网络安全监控中心之间的加密传输。

如上所述的系统，其特征在于：网络安全监控中心可以是由总中心和多个下属分中心连接组成分级中心结构，也可是多个平级的总中心或多级中心连接结构。

本发明所述网络违法行为侦知监控追踪取证应急反应方法，其特征在于：利用现有网络安全产品收集客户端网络安全发生事件的各种要素；对所收集的不同格式的信息进行自动识别并生成标准格式的信息，在客户端信息传输设备与网络安全监控中心相应设备之间建立 VPN 通道或其他加密传输通道，保证网络安全监控中心下传给客户端安全设备的反控指令和客户端信息转换设备上传给网络安全监控中心的采集处理的信息在传输过程中不被第三方非法获取或篡改；所述反控信息包括反控指令、设备升级更新程序和查询指令；网络安全监控中心可以与其他相关系统建立加密传输通道，并且可存储传入的信息；该中心进行整个监控区域的调控和重要数据备份与处理。所述监控中心可以是多个分级式或平级式管理模式；所述信息在存储前将进行分级和加密，并设定保留时限及到期处理方式。

本发明利用各种技术手段侦知网络违法行为，使网络由单点防护发展到系统防护，具体地说，本发明可实现如下效果：

1.使用全面的技术手段侦知网络违法行为并进行防护。采用多种网络安全产品，如防火墙、IDS。利用客户端程序采集这些网络安全产品的日志、报警信息和原始数据包等相关信息，转换成统一格式，与监控应急中心建立加密通道后传递到所属监控应急中心。在建立加密通道时还需要通过预置电子证书或者密码对等方式进行身份认证。

2.能充分支持人工辅助处理，人工辅助是本体系的重要组成分，计算机与人工有机结合可以有效提高网络违法行为识别率，进行及时有效地处理。与人工结合的方式包括：系统对采集的数据进行初步分析发出报警后，人工进行再次分析，减少误报，提高准确性；包括对确认的网络违法行为进行人工处理，

向受到网络违法行为损害的用户提供技术支持和服务。

3.可以进行取证。客户端自动存储侦知网络违法行为时段的原始数据包，并上传中心。在必要时可以传递给国家有关机构存档，如：公安部门、公证部门等，事后作为追查攻击者的依据和追究责任的证据。

4.可以充分利用能够获知的其他信息通过数据挖掘和模式匹配分析追踪网络攻击者的真实网络地址。这些信息包括被攻击用户客户端采集到的信息，包括其他关联客户端采集到的信息，包括第三方提供的信息。所谓其他关联客户端是指：如果网络攻击者用于中转的服务器也属于系统客户端之一监控范围，则监控该服务器的客户端为关联客户端。所谓第三方包括其他政府部门和网络相关公司。

5.可以接收存储多种来源的数据信息，并利用这些数据采用数据挖掘技术获取特定用途的结果。所谓多种来源的数据信息包括不同网络安全产品、不同网络设备、网络服务提供商和其他非网络途径采集的信息，如居民住址、城市地理信息、电话号码登记资料。

6.在对单点进行防护时，充分调动整个系统中的有用信息。

图面说明：

图 1 是本发明的客户端组成示意图。

图 2 是本发明的网络安全监控中心示意图。

图 3 是本发明的跳转主机示意图。

图 4 是本发明的整体系统结构示意图。

图 5 是本发明的客户端安全设备为软件，与客户端信息转换设备安装在同一台设备上的实施例图。

图 6 是本发明的客户端安全设备为硬件，不可与客户端信息转换设备安装在同一台设备上的实施例图。

图 7 是本发明的客户端信息转换设备与客户端安全设备原服务器的连接示意图。

图 8 是本发明所述方法的信息处理流程示意图。

图 9 是本发明所述设备及方法的一种应用实施例示意图。

本发明的具体结构及方法的实施例说明如下：

此安全系统包括网络安全监控中心和客户端两部分。

所谓客户端安装在专用计算机网络中，包括客户端安全设备、客户端信息转换设备和客户端信息传输设备，如图 1 所示。

其中设备 1（客户端安全设备）可以是市场上普通的 IDS、防火墙、网络传输内容监控软件和其他可以产生与网络状况、网络传输内容有关的信息的软硬件产品或模块。这些客户端安全设备可以独立用来对网络进行一定的保护，如：侦知网络攻击、过滤规则不允许的网络传输数据包、找出网络中传输的特

定信息（如：机密、黄色、非法文字或图片）。

在本安全系统中使用时不影响这些客户端安全设备原有功能的实现。该设备提供软件检测网络传输的数据包产生相应信息并做出动作。根据该设备提供软件的不同，可以安装在专用计算机网络中的不同位置。

设备 1（客户端安全设备）也可以是具有某种特殊功能的特别设备，其主要特征是可以产生对安全系统有用的信息，并可以被设备 2（客户端信息转换设备）采集处理。

设备 2（客户端信息转换设备）提供软件实现两个功能，其一是采集设备 1（客户端安全设备）产生的与网络安全相关信息，并将网络安全相关信息转换成网络安全监控中心可以识别的统一格式，然后交给设备 3（客户端信息传输设备）传递给网络安全监控中心。其二是把从设备 3（客户端信息传输设备）接收的来自网络安全监控中心的反控信息转换成设备 1（客户端安全设备）可以识别的格式，然后传递给设备 1（客户端安全设备），实现网络安全监控中心对设备 1（客户端安全设备）的反控。

所谓反控信息包括反控指令、设备升级更新程序、查询指令等。

如网络安全领域技术人员所知，现有网络安全产品一般分单点式和客户端/服务器（或称探头模块/控制台）形式。软件单点式产品一般安装在普通计算机上，在产生网络安全日志信息后，该日志信息可以被读取和分析。硬件单点式产品使用专门硬件，一般有外接控制端口供用户管理系统。客户端/服务器（或称探头模块/控制台）式产品的客户端（探头模块）产生的网络安全相关信息可以被实时传送到服务器（控制台）。该方法使用安装软件程序的方式获取软件单点式网络安全产品产生的信息，利用外接接口获取硬件单点式产品的安全信息。用模拟服务器（控制台）接收并转发客户端（探头模块）信息或者网络监听截取的方式获取客户端/服务器（探头模块/控制台）式产品的安全信息。上述用于获取网络安全产品产生信息的部分（软件或者硬件）统一称为信息采集模块。信息采集方式示意图见图 5、6、7。

这样进行信息采集的好处是不影响用户原有客户端安全设备的正常运行。

如网络安全领域技术人员所知，网络安全产品产生的信息主要包括描述网络安全发生事件的各种要素，如：时间、源 IP、目的 IP、端口、网络协议、事件分类（如非法请求、不正确口令或用户的登录失败、网络攻击、非法信息传递等）、事件安全级别（高中低级或数字量化分级）、事件发生后安全产品自动采取了何种措施等。不同网络安全产品产生的信息内容、协议、编码等不尽相同，同种网络安全产品产生的信息内容、协议、编码等相同，信息采集模块

采集信息后信息处理模块对采集到的信息进行转换，转换为协议、编码等符合统一格式标准的信息。

格式转换的一种参考方式如下：为了最大限度利用信息，取尽量多的网络安全产品，对其产生的信息内容项目进行分类，以这些内容项目的类型全集为标准格式的内容项目分类，并对各种网络安全产品建立映射关系表。设备 2（客户端信息转换设备）可以自动识别不同设备 1（客户端安全设备）的信息，使用对应的协议接受后按映射表读取并生成标准格式的信息。自动识别不同设备 1（客户端安全设备）的功能也可以通过在安装设备 2（客户端信息转换设备）时根据使用的设备 1（客户端安全设备）设定人工实现。

上述格式转换方式不是唯一的，只可以被视为一种可能的举例，不可以视为对本发明的限制。例如可以采用固定内容项目分类，丢弃其他内容项目的转换方式。

设备 3（客户端信息传输设备）提供 VPN 软件或其他类似可建立逻辑安全通道的软件，在客户端信息传输设备与网络安全监控中心相应设备之间建立 VPN 通道或其他加密传输通道，保证网络安全监控中心下传给设备 1（客户端安全设备）的反控指令和设备 2（客户端信息转换设备）上传给网络安全监控中心的采集处理的信息在传输过程中不被第三方非法获取或篡改。

为了保证信息本身的可靠性，还需要对信息做进一步的安全处理。例如：为了防止接收到伪造、篡改或者失真的信息，需要进行发送方和接收方身份的认证、完整性校验、防重放攻击等处理。

如信息安全领域技术人员所知，在信息传递过程中进行安全处理的手段有很多成型的技术处理手段，在此进行部分举例。

数据加密

对于将在通道中传送的信息，将采用密钥长度为 64 bits 到 128 bits 的高强度分组加密算法进行加密处理，以保证信息内容的保密性。

数字文摘

为了保证信息在传输过程中没有被加以篡改，发送方将使用单向变换函数（即哈希函数）对信息进行处理，得到信息的数字文摘 MD1，连同信息本身一起发送给接收方。接收方对收到的信息做同样的处理，得到另外一个数字文摘 MD2，对比 MD1 和 MD2，如果二者不一致即认为该信息是无效的。

时戳

为了防止第三方在网络上截获传输的数据包后重复大量发送（重放攻击），从而导致不能正常处理真实的客户信息请求，发送方发送时将每个信息都加上

时戳，以保证每个信息的唯一性。

一个可能的信息传送过程如下：

发送方

首先向接收方证实自己身份，取得向其发送信息的资格；

将数据采集模块产生的标准信息 M（明文）加上当时的时戳 Tclock，做单向哈希变换，得到该信息的数字文摘 MD1；

用高强度分组密码算法对信息（明文）M 和 MD1 进行加密处理，得到密文结果 C；将密文 C 和当时时戳 Tclock 一起传送给接收方一侧；

接收方

验证向自己发起请求的发送方的身份，验证通过后才进行下一步的处理；

根据和密文 C 同时到达的时戳 Tclock 判断该信息是否已经被处理过；

如果该信息还未被处理，则对密文 C 进行解密处理，用得到的信息明文 M 和时戳 Tclock 做单向哈希变换，将得到的文摘结果 MD2 和信息中自带的文摘 MD1 进行对比，如果二者相同，则认为本次信息有效；

将信息明文 M 传送给后台系统做进一步处理；

信息处理流程示意图见图 8。

设备 3（客户端信息传输设备）可以通过所在的专用计算机网络利用公用网络（如互联网）与网络安全监控中心建立加密通道，也可以利用专线方式与网络安全监控中心建立通道。

设备 2（客户端信息转换设备）和设备 3（客户端信息传输设备）可以组合为一个设备。

一个专用计算机网络中可以有多个设备 1（客户端安全设备）、设备 2（客户端信息转换设备）和设备 3（客户端信息传输设备）。

根据情况，可以一个设备 2（客户端信息转换设备）采集处理多个设备 1（客户端安全设备）产生的信息，也可以每个设备 1（客户端安全设备）有一个设备 2（客户端信息转换设备）负责采集处理。

根据情况，一个设备 3（客户端信息传输设备）可以负责一个或多个设备 2（客户端信息转换设备）与网络安全监控中心之间的加密传输。

网络安全监控（分）中心

本网络安全系统可以采取分级中心结构。所谓分级中心结构，是指系统可以包括总中心和多个下属分中心。每个分中心负责接收一定地理或者网络范围内客户端安全设备产生的信息并进行处理。总中心负责接收所属分中心上传的信息，进行整个监控区域的调控和重要数据备份与处理。可以只有一个总中心，

也可以设立多个平级的总中心。也可以采用一级、二级、三级……的多级中心结构。

分中心负责处理所属用户处的网络安全事件，当分中心由于技术力量、地域等限制不能完全处理该网络安全事件时，可以将该网络安全事件的有关信息上传总中心。总中心的专家协助分中心处理，或者由总中心向涉及该网络安全事件的分中心下达指令，征集该网络安全事件相关信息，指令其他分中心进行配合协助。

总中心的另一个作用是，总中心可以指令各分中心将所属网络事件信息或者符合某一特定条件（如：同一时间段内）的网络安全事件信息上传到总中心，总中心对汇集的信息进行综合分析挖掘，以获得从单一信息很难看出的规律或其他潜在的有价值的信息，（如：网络攻击者的网络跳转路线，追查出网络攻击的真实来源 IP）向相关分中心下达指令，分中心采取行动协助处理。

网络安全监控（分）中心系统包括中心信息传输设备、信息存储设备、中心操作平台设备、信息分析设备、人工支持设备五部分，如图 2 所示。

设备 4（中心信息传输设备）与设备 3（客户端信息传输设备）的功能类似，也提供 VPN 软件或其他类似软件，建立 VPN 通道或其他加密传输通道，保证信息传输安全。设备 3（客户端信息传输设备）和设备 4（中心信息传输设备）的主要区别在于设备 4（中心信息传输设备）提供的软件可以同时与多个设备 3（客户端信息传输设备）建立加密传输通道，向各设备 1（客户端安全设备） 反控信息，接收各设备 2（客户端信息转换设备）上传的信息；而且设备 4（中心信息传输设备）提供的软件还可以与其他中心设备 4（中心信息传输设备）建立加密传输通道，传递各种中心间信息；而且设备 4（中心信息传输设备）还可以与其他相关系统（如公安部门相关系统）建立加密传输通道。

设备 5（中心操作平台设备）可以包括标准计算机、显示设备等组成，并提供相应软件以处理显示其他设备产生的信息，如设备 2（客户端信息转换设备）从用户处转发来的信息，设备 7（信息分析设备）产生的分析结果等。

设备 5（中心操作平台设备）同时还提供软件以允许中心值班操作人员发出查询、反控、删改、复制等操作指令给其他设备。

设备 5（中心操作平台设备）同时还提供软件以允许中心值班操作人员进行发送电子邮件等日常网络应用。

设备 5（中心操作平台设备）同时还提供软件以允许中心值班操作人员在处理显示从设备 2（客户端信息转换设备）获得的信息时，通过设备 4（中心信息传输设备）传递给其他相关部门。

设备 6（信息存储设备）可以由物理存储设施和相应软件构成，用于存储中心接收到的信息以及处理过程中各阶段的结果，存储录入的信息（如：用户资料），存储其他途径获取的资料（如：从公安、电信等部门获取的网络、人员信息；从书籍、报刊、网络获取的背景信息和知识等。

设备 6（信息存储设备）还提供软件以允许这些信息在存储前可以被分级和加密，防止非授权的访问和篡改。

设备 7（信息分析设备）可以由标准计算设备构成。

设备 7（信息分析设备）同时提供软件允许中心值班操作人员通过设备 5（中心操作平台设备）向设备 7（信息分析设备）发出指令，对收集到的全部或者部分指定信息进行分析，或者为了达到指定的目的自动对所有数据进行筛选和分析。为了达到这个目的，设备 7（信息分析设备）同时提供软件以允许设备 7（信息分析设备）查询访问设备 6（信息存储设备）。

为了达到这个目的，设备 7（信息分析设备）提供的软件中可以采用的技术手段包括采用数据挖掘技术通过找出信息间的关联达到发现趋势、追寻网络违法行为来源、发现新型攻击手段等目的。

如计算机领域技术人员所知，所谓数据挖掘就是从大量的、不完全的、模糊的、随机的数据中提取隐含在其中的，人们事先不知道的，但有是潜在有用的信息和知识的过程。包括对数据库中的大量业务数据进行抽取、转换、分析和其他模型花处理，从中获取辅助商业决策的关键性数据。

数据挖掘的目的是从数据库、文件系统或者其他组织在一起的数据集合中提取人们感兴趣的知识。提取的知识表示为概念、规则、规律、模式等形式。

数据挖掘的技术方法包括：统计、关联规则、基于历史的分析、遗传算法、聚集检测、连接分析、决策树、神经元网络等。

设备 8（人工支持设备）用于弥补计算机智能的不足。设备 8（人工支持设备）提供软件允许技术专家对设备 7（信息分析设备）分析处理过的信息进行进一步分析，利用专家的经验加快分析过程，减少失误。

设备 8（人工支持设备）提供软件允许专家根据经验提供各种网络违法行为的特点、案例、处理方式，这些资料分类整理建库存储，形成专家库，允许设备 5（中心操作平台设备）进行访问。

应用举例

为了更好的阐述本发明，下面进行应用举例（见图 9），本例子不可以被视为对本发明的限制。

甲地用户 A 要求将自己纳入本网络安全系统的监控范围。该用户处安装有

某公司的 IDS 产品，该 IDS 产品是本网络安全系统可以兼容的产品类型，可以作为客户端安全设备使用。为了节省投资，用户 A 要求不再加装其他模块或产品作为客户端安全设备。

负责甲地网络安全监控的甲分中心接到用户 A 请求后派技术人员前往安装客户端其他设备。由于该 IDS 系统是硬件客户端/服务器模式的，技术人员在该 IDS 系统的服务器前端安装了设备 2 客户端信息转换设备和设备 3 客户端信息传输模块，并利用客户端信息转换设备提供的软件进行了配置。安装完毕后，甲分中心值班操作人员利用设备 5（中心操作平台设备）录入用户 A 的有关信息并通过设备 4（中心信息传输设备）上传总中心，用户 A 正式受到本网络安全系统的监护。

某日，用户 A 受到不明来源的“泪滴”网络攻击，IDS 系统的客户端检测到并产生报警信息。设备 2（客户端信息转换设备）模拟成 IDS 系统的服务器接收到 IDS 客户端上传的信息，然后模拟成 IDS 系统客户端转发给 IDS 系统服务器，把 IDS 系统服务器返回的信息返回给 IDS 系统客户端。在这过程中，设备 2（客户端信息转换设备）获得了 IDS 系统产生的网络安全有关信息。该 IDS 系统产生的信息（msg0）内容为：事件发生时间：Tattack、网络安全事件分类代码：27（泪滴攻击在该 IDS 系统网络安全事件分类代码表中的代码）、攻击来源：IP2、攻击目的：IPm。设备 2（客户端信息转换设备）将上述内容读出后重新生成统一格式的信息（msg1）：用户 A、事件发生时间 Tattack、网络安全事件分类代码 39（泪滴攻击在本网络安全系统网络安全事件分类代码表中的代码）、攻击来源 IPn、攻击目的 IPm。设备 3（客户端信息传输设备）采用 SSL 协议与预先设定的甲地分中心建立联系，并利用预置的 RSA 公私密钥对证明自己和分中心的身份。将信息明文 msg1 做单向哈希变换，得到该信息的数字文摘 MD1，用 1024 位 DES 加密算法对信息（明文）M 和 MD1 进行加密处理，得到密文结果 C；将密文 C 和当时时戳 Tclock 一起传送给甲分中心。

甲分中心根据和密文 C 同时到达的时戳 Tclock 判断该报警信息还未被处理；对密文 C 进行解密处理，用得到的信息明文 msg1 和时戳 Tclock 做单向哈希变换，将得到的文摘结果 MD2 和信息中自带的文摘 MD1 进行对比，发现二者相同，认为本次信息有效；将信息明文 msg1 传送给设备 6（信息存储设备），信息传输过程结束。

在信息传输过程中，有人企图进行破坏活动，将截获的用户 A 处发出的报警数据包再次发出。甲分中心收到后，发现 Tclock 表明该信息已经被处理过了，丢弃该信息，同时将该情况报告设备 5（中心操作平台设备）。

设备 6（信息存储设备）接收到 msg1 后，根据 msg1 的内容进行分类、分级处理，以便于查询和管理。查询的方式可以包括以时间、用户名称、攻击方式代码、攻击所属级别、目标 IP、来源 IP 等为查询关键字。不同级别的信息可以被拥有不同权限的中心人员进行查阅等操作。

信息在分类处理后采用 1024 位 DES 进行加密，然后将加密生成的密文进行存储，防止非法阅读修改。

设备 6（信息存储设备）接收分类分级处理后，信息被存储的同时，报警信息 msg1 在设备 5（中心操作平台设备）上显示出来：T 时间，A 用户受到 39 号攻击，攻击最终来源 IP2， 目的 IPm 等。操作人员可以查询设备 6（信息存储设备）中存储的所有与 msg1 相关的信息，如：A 用户的信息、有关 39 号攻击的有关资料、IP 相关信息等。操作人员根据资料认为攻击最终来源 IP2 不在甲分中心职权范围，于是操作人员在设备 5（中心操作平台设备）上进行操作，将该攻击的有关信息和背景资料传递给本地（甲分中心）的设备 8（人工支持设备）和外地的总中心。在甲分中心设备 8（人工支持设备）值班的智能专家在设备 8（人工支持设备）上看到这次攻击的有关资料，认为这是一次较严重的攻击，需要立即采取行动阻止攻击造成损害。专家立即通过电话和电子邮件与 A 用户的有关人员进行联系，通报这次攻击，同时根据自己的专业知识和设备 6（信息存储设备）中保存的有关 39 号攻击的参考处理方案，远程指导用户 A 处的网络管理人员采取应急措施，并派专人前往用户 A 处现场协助用户处理。由于该攻击的严重性，甲分中心同时把信息传递给甲地有关公安部门备案。

总中心与分中心之间、分中心与有关公安部门之间网络传输的信息也通过信息传输设备传输。

总中心接收到甲分中心传来的报警信息后，解密还原，获得的信息包括：信息级别：高、信息类型：实时求助、用户上报的信息 msg1、用户 A 的有关资料等。总中心的设备 5（中心操作平台设备）上立刻显示该信息，值班人员判断后转交总中心设备 8（人工支持设备）。总中心设备 8（人工支持设备）值班的专家接到报警后，利用自身专业知识和总中心设备 6（信息存储设备）中资料判断该警情需要注意的处理细节，通过电话或者网络与甲分中心专家进行指导，必要时直接与用户联系。

同时，总中心专家根据总中心设备 6（信息存储设备）中来自电信的 IP 地址信息确认 IP2 属于乙地乙分中心监控范围，于是将该报警信息转发到乙分中心，指令乙分中心密切监控 IP2，并将该有关 IP2 的信息上传总中心。乙分中心接收到总中心指令后，查找到 IP2 属于用户 B 的网络，于是通过网络向负责

监控用户 B 的设备 1（客户端安全设备）随时上报用户 B 的有关信息作为回应，并将来自用户 B 的回应信息上传总中心。用户 B 的回应信息包括用户 B 网络中服务器的登录日志等。

总中心专家利用设备 8（人工支持设备）对来自用户 B 的回应信息和用户 A 的报警信息进行分析，发现网络攻击者将用户 B 的服务器作为跳转主机，以达到隐藏自己真实 IP 来源的目的，其登录跳转主机时使用的 IP1 属于丙分中心监控范围，于是指令丙分中心协助调查。

丙分中心发现 IP1 所属单位 C 不是本系统的用户，于是派专人前往该单位请求协助。经同意，丙分中心专家在 C 单位的网络上实时人工操作搜寻有关信息，并安装了临时设备 1（客户端安全设备）等模块。经努力，发现单位 C 的服务器也成为了跳转主机。经总中心分析，获取其登录跳转主机时使用的 IP0。

再次查询电信提供的 IP 资料，发现 IP0 为一 ISP 提供给拨号用户使用的 IP。于是将这一情况通知了该 ISP，ISP 根据自己的系统记录，证实事件发生时使用 IP0 的用户上网使用的电话的号码为 87654321，于是将这一情况反馈给网络安全监控应急总中心，并将该情况通知有关部门。

有关部门根据总中心、电信部门、ISP 等单位提供的信息，采取进一步行动。

总中心在征求事件有关各方的意见后，将上述情况中的部分内容通知用户 A、B、C，并根据其网络在该次事件中表现出来的网络安全问题提出网络安全建议，协助用户实施。

说 明 书 附 图

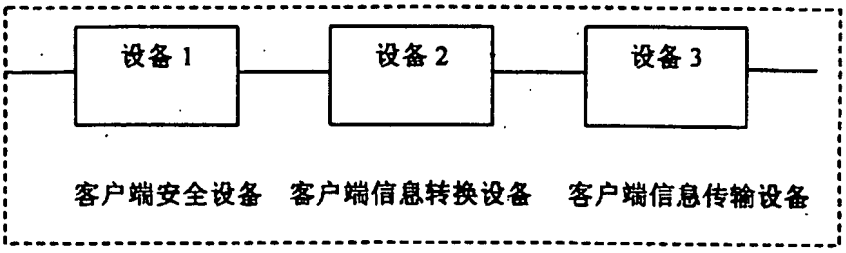


图 1

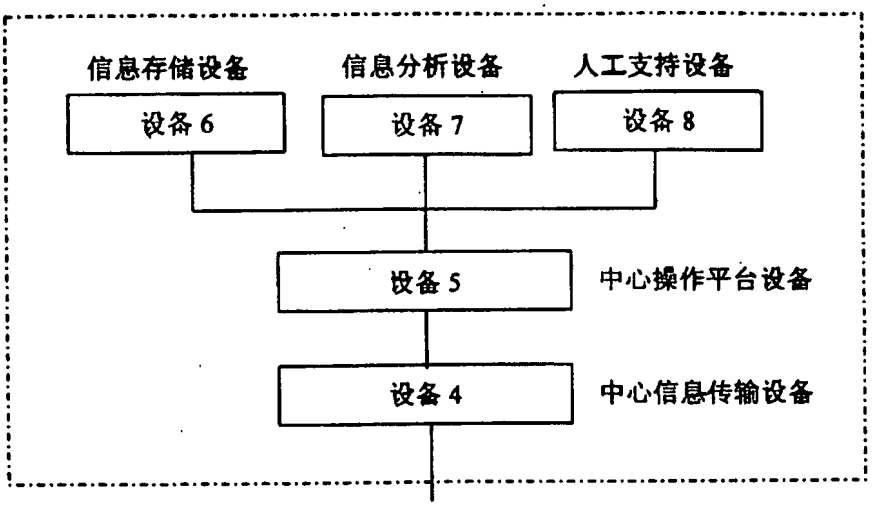


图 2

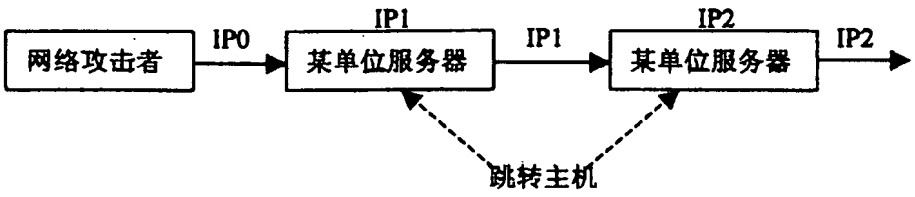


图 3

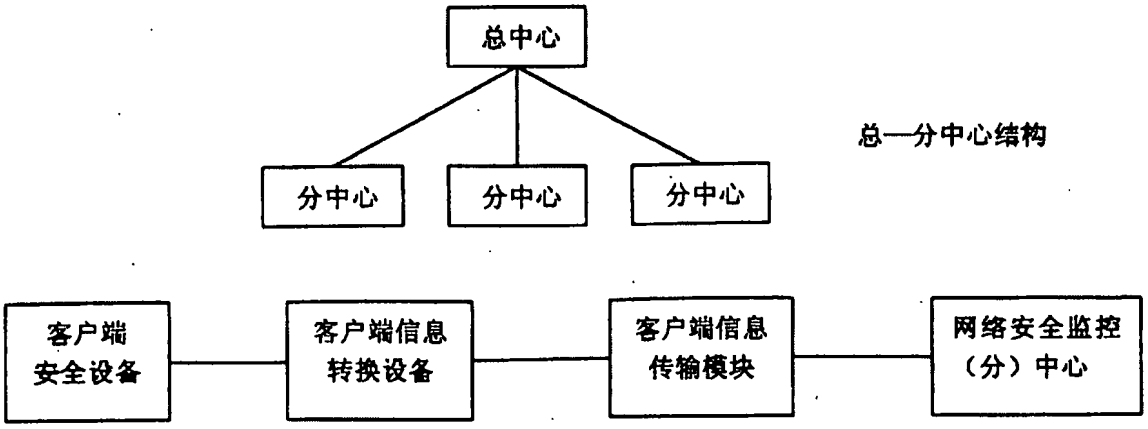

总中心
分中心
分中心
分中心
总—分中心结构
客户端
安全设备
客户端信息
转换设备
客户端信息
传输模块
网络安全监控
（分）中心

图4

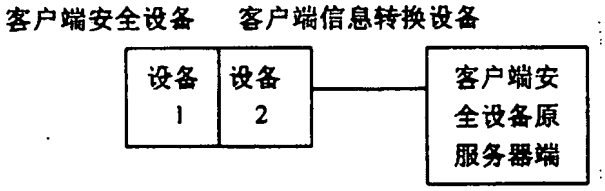

客户端安全设备
客户端信息转换设备
设备
1
设备
2
客户端安
全设备原
服务器端

图5

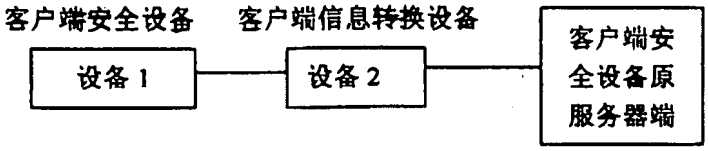

客户端安全设备
客户端信息转换设备
设备 1
设备 2
客户端安
全设备原
服务器端

图6

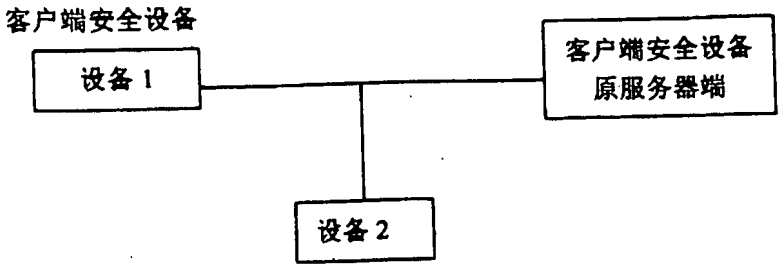

客户端安全设备
设备 1
客户端安全设备
原服务器端
设备 2

图7

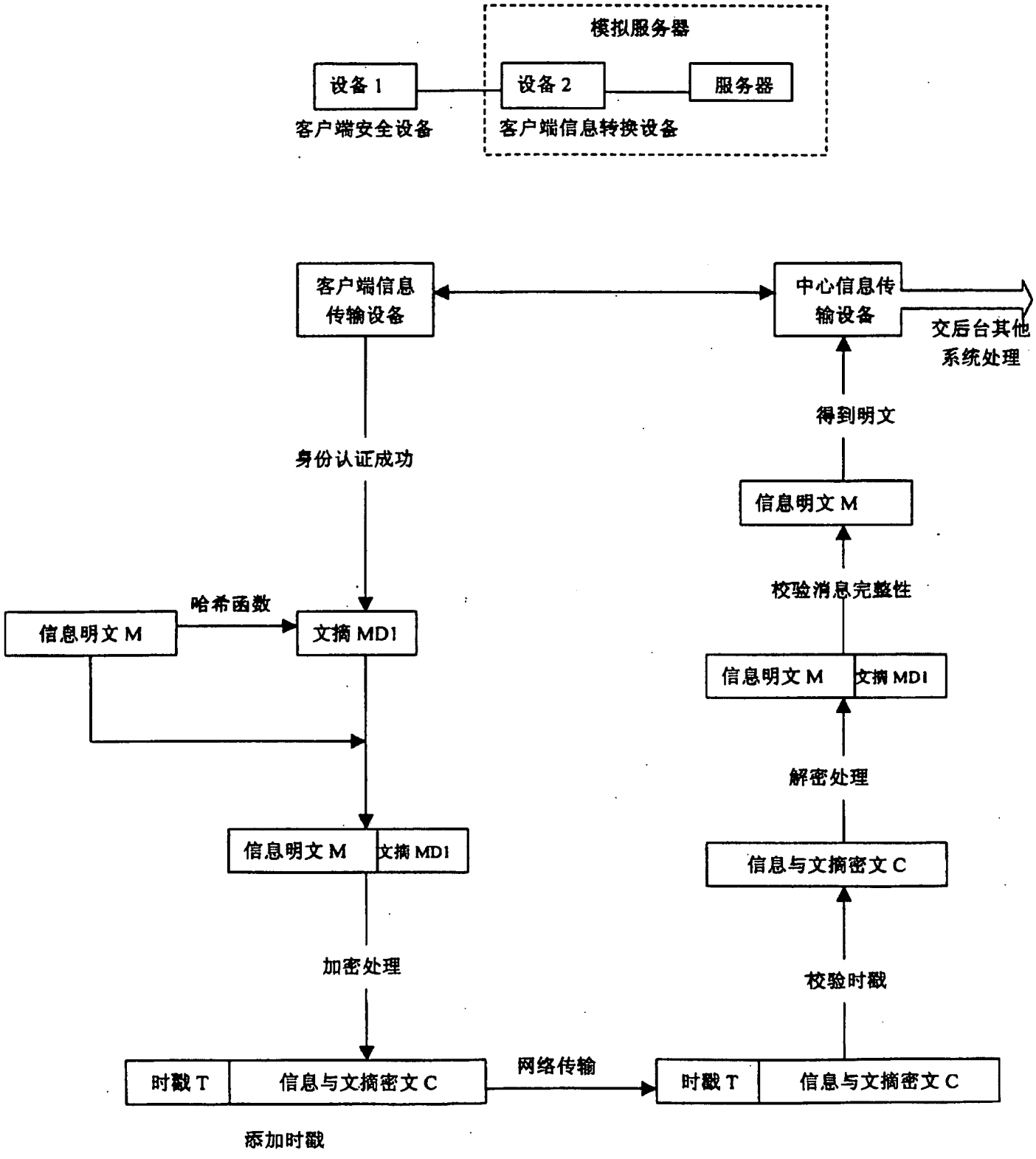

模拟服务器
设备 1
设备 2
服务器
客户端安全设备
客户端信息转换设备
客户端信息传输设备
中心信息传输设备
交后台其他系统处理
得到明文
身份认证成功
信息明文 M
校验消息完整性
哈希函数
信息明文 M
文摘 MD1
信息明文 M
文摘 MD1
解密处理
信息明文 M
文摘 MD1
信息与文摘密文 C
加密处理
校验时戳
时戳 T
信息与文摘密文 C
网络传输
时戳 T
信息与文摘密文 C
添加时戳

图 8

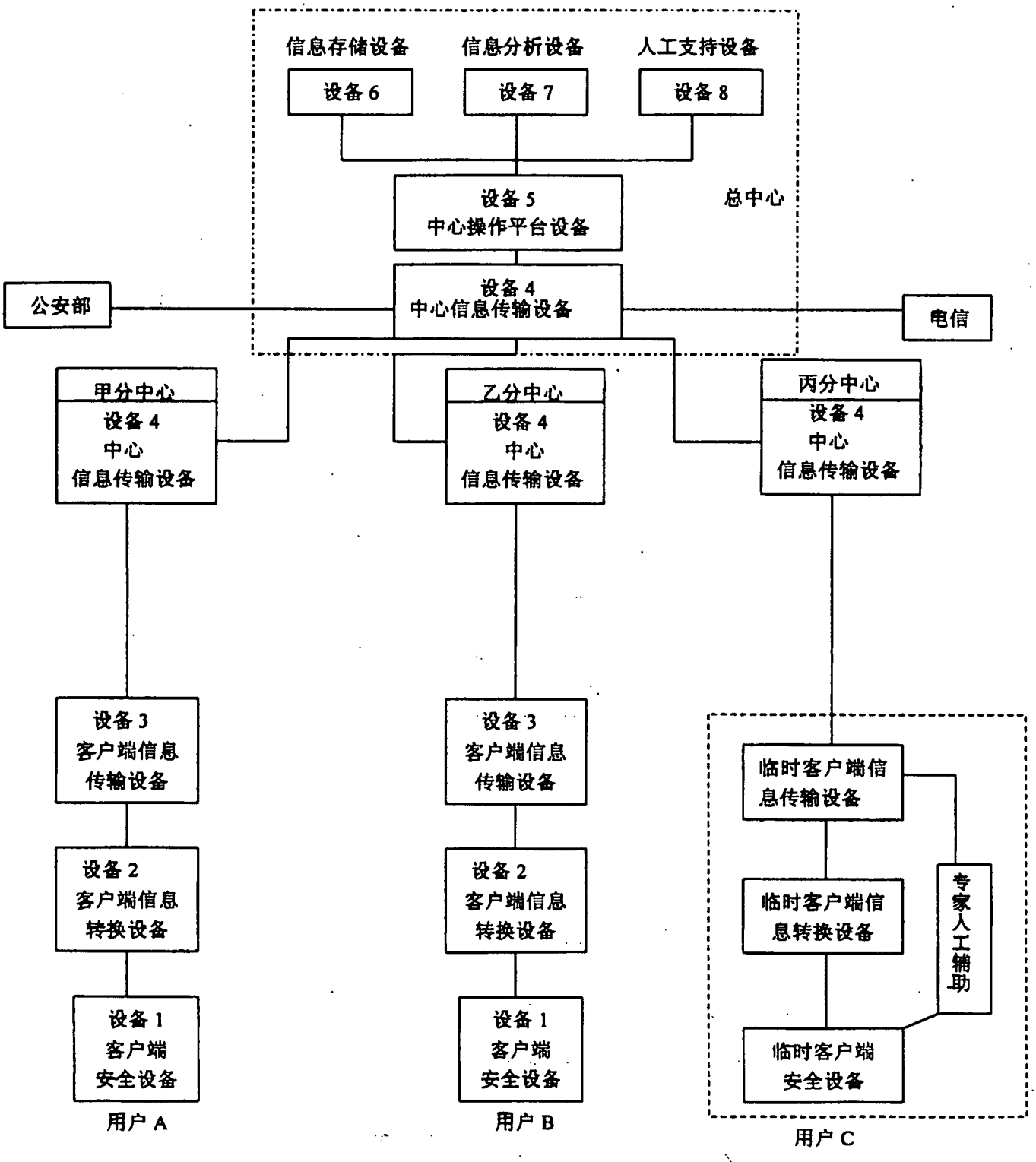

信息存储设备
信息分析设备
人工支持设备
设备 6
设备 7
设备 8
设备 5
中心操作平台设备
总中心
公安部
设备 4
中心信息传输设备
电信
甲分中心
设备 4
中心
信息传输设备
乙分中心
设备 4
中心
信息传输设备
丙分中心
设备 4
中心
信息传输设备
设备 3
客户端信息
传输设备
设备 2
客户端信息
转换设备
设备 1
客户端
安全设备
用户 A
设备 3
客户端信息
传输设备
设备 2
客户端信息
转换设备
设备 1
客户端
安全设备
用户 B
临时客户端信
息传输设备
临时客户端信
息转换设备
临时客户端
安全设备
专家人工辅助
用户 C

图 9